Commentary
Volume 16:2, 2023

Journal of Computer Science & Systems Biology

ISSN: 0974-7230

Open Access

Enhancing Data Security and Privacy in Cloud Computing through Homomorphic Encryption

Jones Fullerton*

Department of Business Information Systems, University of Calgary, Calgary, Canada

Description

Cloud computing has revolutionized the way data is stored, processed, and accessed. However, concerns over data security and privacy have emerged as significant challenges in this paradigm. Traditional encryption techniques fall short in cloud environments, as data needs to be decrypted for processing, increasing the risk of unauthorized access. Homomorphic encryption, a promising cryptographic solution, allows for performing computations on encrypted data without the need for decryption. This article explores the concept of homomorphic encryption and its potential to enhance data security and privacy in cloud computing. We discuss its working principles, benefits, and current research advancements in this field. Furthermore, we highlight the challenges and future directions for the adoption of homomorphic encryption in cloud computing. Cloud computing offers numerous advantages, such as scalability, cost-efficiency, and accessibility. However, it also introduces vulnerabilities concerning data security and privacy. Traditional encryption techniques, while effective in protecting data during transmission and storage, become a hindrance when it comes to processing data in the cloud. Homomorphic encryption presents a viable solution by allowing computations on encrypted data, thereby preserving confidentiality and privacy. This article presents an overview of homomorphic encryption and its potential to address data security concerns in cloud computing [1-3].

Homomorphic encryption

Homomorphic encryption is a cryptographic technique that enables computations on encrypted data without the need for decryption. It allows cloud service providers to perform operations on encrypted data, preserving the confidentiality of sensitive information. The three main types of homomorphic encryption are partially homomorphic encryption (PHE), somewhat homomorphic encryption (SHE), and fully homomorphic encryption (FHE). Each type offers varying degrees of computational capabilities while maintaining data privacy.

Homomorphic encryption offers several benefits for enhancing data security and privacy in cloud computing

Confidentiality: With homomorphic encryption, data remains encrypted throughout its lifecycle in the cloud. This ensures that even during computations and processing, sensitive information remains confidential and protected from unauthorized access.

Privacy: Homomorphic encryption allows data owners to delegate data processing tasks to the cloud while preserving the privacy of their data. Cloud service providers can perform computations on encrypted data without having access to the plaintext, maintaining the privacy of user data.

Outsourced computation: Homomorphic encryption enables secure outsourcing of computations to the cloud. Data owners can delegate complex calculations to the cloud without revealing the actual data, making it ideal for scenarios where data confidentiality is crucial.

Current research advancements

Significant progress has been made in the field of homomorphic encryption, addressing its limitations and improving its efficiency. Researchers have developed novel homomorphic encryption schemes, such as the BGV (Brakerski-Gentry-Vaikuntanathan) scheme and the CKKS (Cheon-Kim-Kim-Song) scheme, which offer better performance and increased computational capabilities. Additionally, advancements in hardware acceleration techniques, such as the use of specialized processors like secure enclaves and trusted execution environments, have improved the efficiency of homomorphic encryption.

Challenges and future directions

Despite the promising potential of homomorphic encryption, several challenges need to be addressed for its widespread adoption in cloud computing. These challenges include performance limitations, scalability issues, and the need for standardized implementations and protocols [4,5]. Future research efforts should focus on developing more efficient homomorphic encryption schemes, optimizing performance, and establishing industry-wide standards to facilitate seamless integration of this technology into cloud computing platforms.

Homomorphic encryption offers a viable solution to enhance data security and privacy in cloud computing. By allowing computations on encrypted data, it enables data owners to delegate processing tasks to the cloud while preserving confidentiality. Although challenges remain, ongoing research and advancements in homomorphic encryption are paving the way for its wider adoption in cloud computing. As homomorphic encryption continues to evolve, it has the potential to reshape the landscape of data security and privacy, providing a robust and efficient solution for protecting sensitive information in cloud environments.

Acknowledgement

None.

Conflict of Interest

Authors declare no conflict of interest.

References

1. Regev, Oded. "On lattices, learning with errors, random linear codes, and cryptography." *J ACM* 56 (2009): 1-40.
2. Al Badawi, Ahmad, Louie Hoang, Chan Fook Mun and Kim Laine, et al. "Privft: Private and fast text classification with homomorphic encryption." *IEEE Access* 8 (2020): 226544-226556.
3. Jung, Wonkyung, Sangpyo Kim, Jung Ho Ahn and Jung Hee Cheon, et al. "Over 100x faster bootstrapping in fully homomorphic encryption through memory-centric optimization with gpus." *IACR Trans Cryptogr Hardw Embed Syst* (2021): 114-148.
4. Mert, Ahmet Can, Sunmin Kwon, Youngsam Shin and Donghoon Yoo, et al. "Medha: Microcoded hardware accelerator for computing on encrypted data." *arXiv preprint arXiv* 2210.05476 (2022).
5. Duong-Ngoc, Phap, Sunmin Kwon, Donghoon Yoo and Hanho Lee. "Area-efficient number theoretic transform architecture for homomorphic encryption." *IEEE Trans Circuits Syst I Regul Pap* 70 (2023) 1270–1283.

****Address for Correspondence:*** *Jones Fullerton, Department of Business Information Systems, University of Calgary, Calgary, Canada, E-mail: JonesFullerton2@yahoo.com*

Received: 01 February, 2023, Manuscript No. jcsb-23-99473; **Editor Assigned:** 03 February, 2023, Pre QC No. P-99473; **Reviewed:** 14 February, 2023, QC No. Q-99473; **Revised:** 20 February, 2023, Manuscript No. R-99473; **Published:** 27 February, 2023, DOI: 10.37421/0974-7230.2023.16.460

How to cite this article: Fullerton, Jones. "Enhancing Data Security and Privacy in Cloud Computing through Homomorphic Encryption." *J Comput Sci Syst Biol* 16 (2023): 460.